Who is responsible for data processing in smart homes? Reconsidering joint controllership and the household exemption

Who is responsible for data processing in smart homes? Reconsidering joint controllership and the household exemption

Jiahong Chen[*], Lilian Edwards[**], Lachlan Urquhart[***], and Derek McAuley[****]

Key Points

- The growing industrial and research interest in protecting privacy and fighting cyberattacks for smart homes has sparked various innovations in security- and privacy-enhancing technologies (S/PETs) powered by edge computing. The complex technical set-up has however raised a whole series of legal issues surrounding the regulation of smart home with data protection law.
- To determine how responsibility and accountability should be fairly assumed by stakeholders, there is a pressing need to first clarify the roles of these parties within the existing data protection legal framework. This article focuses on two legal concepts under the General Data Protection Regulation (GDPR) as the mechanisms to (dis)assign responsibilities to various categories of entities in a domestic Internet of Things (IoT) context: joint controllership and the household exemption.
- A close examination of the relevant provisions and case-law shows a widening notion of joint controllership and a narrowing scope for the household exemption. While this interpretative approach may prevent evasion of accountability in specific cases, it may lead to the unintended consequence of imposing disproportionate compliance burdens on developers, contributors, and users of smart home safety technologies. By discouraging users to adopt S/PETs, data protection law may likely lead to a lower level of privacy and security protection.
- The differential responsibilities among joint controllers as envisaged in case-law may reconcile the tensions to some degree, but certain limitations remain. The regulatory dilemma in this regard highlights some underlying assumptions of data protection law that are no longer valid with regard to a smart home, and thus calls for further conceptual and empirical studies on fair reassignment of responsibility and accountability in a domestic IoT setting.

* Jiahong Chen, Horizon Digital Economy Research, University of Nottingham, Nottingham, UK

** Lilian Edwards, Newcastle Law School, Newcastle University, Newcastle, UK

*** Lachlan Urquhart, School of Law, University of Edinburgh, Edinburgh, UK

**** Derek McAuley, Horizon Digital Economy Research, University of Nottingham, Nottingham, UK

This work was supported by the Engineering and Physical Sciences Research Council [grant numbers EP/M02315X/1, EP/N028260/2, EP/R03351X/1].

Introduction: towards a safer home built by many

Smart home Internet of Things (IoT) devices are notoriously badly secured. Commercial practices geared towards usability see devices shipped with default passwords, but users rarely change these. This has led to cases of IP connected cameras being remotely accessible via search engine Shodan, enabling babies to be monitored sleeping.[1] Similarly, poorly secured devices can be more vulnerable to remote access attacks, implicating them in botnets. We have seen this in the case of the Mirai,[2] Persirai[3] and Reaper[4] botnets.[5] Concurrently, there are growing concerns about the personal data-driven economy resulting from new compliance requirements and high fines under the General Data Protection Regulation (GDPR).[6] A key issue is the dominant cloud-based big data analytics infrastructure dominating IoT product and service design. It enables creation of cheaper devices with data collected locally, analysed remotely, and the service provided locally again.[7]

These IoT privacy and security concerns have sparked a growing research agenda in creating local data storage and analysis infrastructures, where data analytics is brought to the data, as opposed to centralizing the data. This provides users more control over who accesses their data, why, for how long, and so forth. From a regulatory perspective, the European Data Protection Supervisor (EDPS) has extolled the virtues of such personal information management systems (PIMS) sitting at the edge of the network,[8] as has a recent Royal Society report.[9]

Development and adoption of security- and privacy-enhancing technologies (S/PETs) are not just priorities on the EU's Digital Single Market Strategy,[10] but indeed encouraged or even required by the GDPR.[11] Yet, the uptake of these technologies will depend on a suitable legal environment with appropriate regulatory incentives provided for developers and users of such technologies and without imposing excessive compliance burdens on them. We however have concerns over the potential impact of data protection law on S/PETs in a domestic IoT context, especially considering how responsibility and accountability are assigned to various groups of actors under the current legal framework. The notion of joint controllers and the household exemption are therefore of significant relevance as they serve as the GDPR's primary mechanisms to identify the parties responsible to ensure data protection requirements are met.

To illustrate the implications of joint controllership and the household exemption for domestic IoT S/PETs with edge computing solutions, this article will look at two ongoing research initiatives. The Databox project (funded by the UK's Engineering and Physical Sciences Research Council, EPSRC) demonstrates how data protection principles can be built into data processing architectures by design.[12] With personal data stored and analysed on a local PIMS, Databox aims to enable users to benefit from the use of their data without compromising their data privacy. Work by Urquhart et al. considers how it enables accountability, as required in Article 5(2) of the GDPR, by providing mechanisms both for substantive compliance, but also

1 Leo Kelion, 'Trendnet Security cam Flaw exposes Video Feeds on Net' (*BBC*, 8 March 2012) <https://www.bbc.co.uk/news/technology-16919664> accessed 9 December 2019.

2 Monty Munford, 'Could your "smart" Home be a Weapon of Web Destruction?' (*BBC*, 28 October 2016) <https://www.bbc.co.uk/news/business-37776964> accessed 9 December 2019.

3 Danny Palmer, '120,000 IoT Cameras Vulnerable to New Persirai Botnet Say Researchers' (*ZDNet*, 10 May 2017) <https://www.zdnet.com/article/120000-iot-cameras-vulnerable-to-new-persirai-botnet-say-researchers/> accessed 9 December 2019.

4 John Leyden, 'Do Fear the Reaper: Huge Army of Webcams, Routers Raised from 'one million' Hacked Orgs' *The Register* (20 October 2017) <https://www.theregister.co.uk/2017/10/20/iot_reaper_botnet_growing_fast/> accessed 9 December 2019.

5 See also European Union Agency for Cybersecurity, *ENISA Threat Landscape Report 2018* (2019) <https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018> accessed 9 December 2019.

6 Mark Sweney, 'Marriott to be Fined Nearly £100m over GDPR Breach' *The Guardian* (9 July 2019) <https://www.theguardian.com/business/2019/jul/09/marriott-fined-over-gdpr-breach-ico> accessed 9 December 2019.

7 Lachlan Urquhart, Tom Lodge and Andy Crabtree, 'Demonstrably Doing Accountability in the Internet of Things' (2019) 27(1) International Journal of Law and Information Technology 1.

8 European Data Protection Supervisor, *EDPS Opinion on Personal Information Management Systems* (2016).

9 The Royal Society, *Protecting privacy in practice: The current use, development and limits of Privacy Enhancing Technologies in data analysis* (2019) <https://royalsociety.org/-/media/policy/projects/privacy-enhancing-technologies/privacy-enhancing-technologies-report.pdf> accessed 9 December 2019.

10 Commission, 'A Digital Single Market Strategy for Europe' (2015) Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions COM(2015) 192 final; Commission, 'Mid-Term Review on the implementation of the Digital Single Market Strategy: A Connected Digital Single Market for All' (2017) Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions COM(2017) 228 final.

11 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1 ('GDPR'), arts 5(1)(a), (c), (e), (f), 24, 25, Recital 78.

12 Richard Mortier and others, 'Personal Data Management with the Databox: What's Inside the Box?' (2016 ACM Workshop on Cloud-Assisted Networking, Irvine, California, 12 December 2016).

demonstrating compliance.[13] Another EPSRC-funded project, Defence Against Dark Artefacts (DADA),[14] addresses smart home cybersecurity risks by identifying strategies for providing security threat management at the edge of the network. This is achieved by screening the behaviour of devices on the network, and detecting when activity is abnormal. If data flows are going to unexpected destinations or exhibiting abnormal patterns, this may indicate threat actors with remote access or stealing information.[15]

The development and operation of both Databox and DADA, however, relies heavily on the collection and analysis of device data (which may turn out to be personal or even sensitive data) and involve a wide range of actors who may or may not be categorized as data controllers or data subjects.[16] The complexity of legal relationships in IoT has been highlighted in the literature,[17] and S/PETs will only further increase such complexity. Stakeholders surrounding such systems include *architectural developers* (eg Databox and DADA developers), *third-party component builders* (service/app/driver providers), *device manufacturers* and *users*, while *homeowners*, *family members*, *neighbours* and *visitors* may be affected. All these complexities pose pressing questions in both theoretical and practical terms about how responsibilities are managed, and who the different stakeholders are.

In a scenario where, for example, a homeowner has set up the smart home with such an S/PET solution, should they be treated as a (joint) data controller? If so, can they reasonably claim they are exempted from the controller obligations on the basis of a purely household activity? What about the other involved parties, such as developers of the S/PET system? Fundamentally, and as will be shown below, these questions may eventually come down to the fair allocation of data protection responsibility and accountability among a range of stakeholders. Edge computing for smart homes holds great promise with its architecture designed to keep the use of personal data inside the home, but it remains unclear whether using such technologies would turn homeowners into liable joint controllers. As the rest of this article will show, the way joint controllers and the household exemption have been construed in case-law—with the intention to provide seamless protection to data subjects—may end up running counter to this objective by creating deterrence against the uptake of S/PETs such as Databox and DADA.

Joint controllership: everyone is a data controller?

In ascertaining who is responsible for what sorts of data protection obligations, the first step is always to identify the data controller, or controllers. Under the accountability principle of the GDPR, data controller is the one ultimately responsible for compliance of data protection law.[18] While other categories of actors, such as data processors or —as will be explained below—developers of data processing systems, also play a role in ensuring all data protection principles are observed, the major burdens fall on data controllers.

The GDPR has maintained the same definition of data controller as under the Data Protection Directive (DPD), which is 'the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data'.[19] It follows that, although the GDPR has introduced a number of new provisions on (joint) controllership, there is no reason to assume that the case-law handed down by the Court of Justice of the EU (CJEU) or the opinions issued by the Article 29 Working Party (A29 WP, now the European Data Protection Board, EDPB) at the time of the DPD are no longer relevant, except where they are clearly contrary to the new rules. In fact, it would be helpful to review how the scope of data controller and the notion of joint controllership have been interpreted by the Court and the WP, which would shed further light on how the GDPR is likely to apply to future cases involving a spectrum of stakeholders around

13 Urquhart, Lodge and Crabtree (n 7).

14 Horizon Digital Economy Research, 'Defence Against Dark Artefacts' <https://www.horizon.ac.uk/project/defence-against-dark-artefacts/> accessed 9 December 2019.

15 Sandra Siby, Rajib Ranjan Maiti and Nils Ole Tippenhauer, 'IoTScanner: Detecting Privacy Threats in IoT Neighborhoods' (3rd ACM International Workshop on IoT Privacy, Trust, and Security, Abu Dhabi, 2 April 2017); Ayyoob Hamza and others, 'Clear as MUD: Generating, Validating and Applying IoT Behavioral Profiles' (2018 Workshop on IoT Security and Privacy, Budapest, 20 August 2018).

16 Jenna Mäkinen, 'Data Quality, Sensitive Data and Joint Controllership as Examples of Grey Areas in the Existing Data Protection Framework for the Internet of Things' (2015) 24(3) Information & Communications Technology Law 262.

17 Rolf H Weber and Romana Weber, *Internet of Things: Legal Perspectives* (Springer, Berlin 2010); Guido Noto La Diega and Ian Walden, 'Contracting for the "Internet of Things": Looking into the Nest' (2016) 7(2) European Journal of Law and Technology; Luca Bolognini and Paolo Balboni, 'IoT and Cloud Computing: Specific Security and Data Protection Issues' in Sébastien Ziegle (ed), *Internet of Things Security and Data Protection* (Springer, Cham 2019).

18 GDPR, art 5(2).

19 Ibid art 4(7). See also Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31 ('DPD'), art 2(d).

smart home technical solutions like Databox and DADA. As will be shown in the rest of this section, while various guidance documents issued by EU regulators exhibit a stronger focus on scenarios where joint controllership arises from legal arrangement between controllers, CJEU case-law has broadened the possibility by considering situations where controllers are aligned merely by technical or organizational configurations.

Guidance by European regulators: joint controllership by legal arrangement

When assessing the nature of controllership with regard to a particular entity, one would need to address two key issues: (i) What makes an entity a data controller instead of a mere data processor or even just a 'facilitator'; (ii) What makes two or more entities *joint* controllers rather than independent, sole controllers for different processing operations. Indeed, these are among the major topics covered by the A29 WP's 2010 Opinion on the concepts of controller and processor.[20] Such distinctions are of important legal significance in that, on the one hand, data controllership means the assumption of the primary responsibilities for compliance with data protection law,[21] and on the other, joint controllership means they are under the obligation to make arrangements for shared responsibilities and might be held jointly liable for the entirety of data processing.[22]

The first question regarding the distinction between data controller and data processor is certainly of theoretical and practical significance to protecting personal data in a domestic IoT context, not least because of the cloud-based approach prevalent in the design of many IoT devices, which leads to the ongoing debate about the role of cloud providers as data processors.[23] Importance as this issue is, it falls outside of the main focus of this article and should be a subject matter for future research.

The second question, which is more relevant to the inquiry of this article, concerns the conditions for a group of entities to become *joint* controllers. The WP points out from the outset of the Opinion that 'pluralistic control' is possible and may take a wide variety of forms.[24] The interactions between joint controllers may reflect 'a very close relationship (sharing, for example, all purposes and means of a processing) or a more loose relationship (for example, sharing only purposes or means, or a part thereof)'.[25] However, the mere existence of cooperation between different entities do not necessarily render them joint controllers.[26] Rather, they can be independent (sole) controllers responsible only for their part of the data processing chain.[27] That said, it is also stressed that the assessment must also take into consideration whether 'at macro-level' the processing operations form a 'set of operations' with joint purposes and means.[28] This is particularly likely to be the case when the involved parties have set up shared infrastructures to process personal data.[29]

The examples and discussions throughout the Opinion show that what the WP envisages as joint controllership relies on a legal arrangement whereby 'clear and equally effective allocation of obligations and responsibilities' can be established between controllers. Even when the formal agreement between controllers do not reflect the actual legal relationship (eg designating one party as a data processor while it actually exercises control under the agreement), the substance of such an agreement, accordingly to the Opinion, nevertheless serves as an important indication of the 'contractual arrangements' or 'factual circumstance' against which the validity of appointment of (joint) controllers, as well as their respective responsibilities, is assessed.[30]

Such a 'joint controllership by legal arrangement' approach is also mirrored in a latest EDPB guidance, requiring that '[w]henever joint controllership is envisaged, the parties must apportion in a clear and transparent way their respective responsibilities vis-à-vis the data subject'.[31] Likewise, the discussion in the recent EDPS guidelines on the concepts of controller, processor and joint controllership focuses heavily on scenarios where 'by entering into [an] agreement, the parties commonly determine (or converge on) the purpose and essential elements of the means'.[32] It should be noted that the EDPS's analysis is conducted under Regulation

20 Art 29 Data Protection Working Party, 'Opinion 1/2010 on the concepts of "controller" and "processor"' (2010) 00264/10/EN WP 169.

21 DPD, art 6(2); GDPR, art 5(2).

22 GDPR, arts 26(3), 82(4). See also art 29 Data Protection Working Party (n 20) 22.

23 Art 29 Data Protection Working Party, 'Opinion 05/2012 on Cloud Computing' (2012) 01037/12/EN WP 196; W. Kuan Hon, Christopher Millard and Ian Walden, 'Who is Responsible for "Personal Data" in Cloud Computing?—The Cloud of Unknowing, Part 2' (2012) 2(1) International Data Privacy Law 3; Bolognini and Balboni (n 17).

24 Art 29 Data Protection Working Party, 'Opinion 1/2010 on the concepts of "controller" and "processor"' (n 20) 18.

25 Ibid 19.

26 Ibid 20.

27 Ibid 19.

28 Ibid 20.

29 Ibid 20–21.

30 Ibid 11–12, 17–24.

31 European Data Protection Board, 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default' (2019) 15.

32 European Data Protection Supervisor, 'EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725' (2019) 22–26.

2018/1725, which governs processing of personal data by EU institutions,[33] rather than the GDPR. However, given the similarity in substance and terminology between the two Regulations,[34] it remains helpful in revealing the perceptions of EU data protection regulators towards the notion of joint controllership under the GDPR.

To sum up, the interpretative approach taken by European regulators has placed significant emphasis on the co-decision made between actors involved in the data processing in question when ascertaining their legal status. It is even suggested that data controllers can be 'appointed' by means of legal arrangements, although such an appointment, without prejudice to the data subject's rights against each of them,[35] should be 'null and void' if the designated party does not actually exercise effective control over the processing.[36] Moreover, the joint responsibilities are considered a matter that should 'be determined in principle by controllers' as long as the rights of data subjects remain fully respected.[37]

From *Google Spain* to *Fashion ID*: joint controllership by technical and organizational configurations

Four years after the WP's Opnion, the CJEU had the opportunity to examine the concept of data controller in the high-profile *Google Spain* case.[38] In answering the question referred by the national court as to whether Google constitutes a data controller by operating a search engine that indexes and presents as results the webpages that contain personal data, the Court examines the role of Google in the spreading of information on the Internet. It has come to the conclusion that Google 'plays a decisive role in the overall dissemination of those data in that it renders the latter accessible to any internet user making a search on the basis of the data subject's name, including to internet users who otherwise would not have found the web page on which those data are published'.[39] Also, for the first time, the Court has declared that both the letter and the spirit of data protection law necessitates a broad definition of data controller to ensure 'effective and complete protection of data subjects',[40] which, as will be shown below, has been consistently reiterated by the Court in later decisions.

While the Court has not directly dealt with the issue of joint controllers in this case, an interesting remark was made about how joint controllership may possibly stem from technical configurations. To explain why a website's ability to opt out from Google's indexing (with the 'robots.txt' protocol or the 'noindex' code) does not mean Google does not exercise control over the processing of data, the Court notes that 'even if that option for publishers of websites were to mean that they determine the means of that processing jointly with [Google], this finding would not remove any of the latter's responsibility'.[41] While stated in a purely hypothetical manner, this observation seems to suggest that it is possible for a website to become a joint controller with Google simply by using (or not using) certain technical settings.

The possibly loose relationships between joint controllers are also recognized in *Wirtschaftsakademie*, where the Court rules that the administrator of a Facebook fan page is a joint controller with Facebook.[42] It is reasoned that 'the administrator of a fan page hosted on Facebook, by creating such a page, gives Facebook the opportunity to place cookies on the computer or other device of a person visiting its fan page'.[43] It is also pointed out that the administrator 'has an influence on the processing of personal data' by 'defin[ing] the criteria in accordance with which the statistics are to be drawn up and even designat[ing] the categories of persons whose personal data is to be made use of by Facebook', which 'contributes to the processing of the personal data of visitors to its page'.[44]

While the Court took note of the potential contractual relationship between a fan page administrator and Facebook, this did not play a substantial role in the Court's analysis.[45] Rather, the focus was entirely on how the setting up of fan page would technically facilitate Facebook to collect personal data from its users. Hence, it becomes clear that, through *Google Spain* and *Wirtschaftsakademie*, the Court has established what we

33 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC [2018] OJ L295/39.

34 See, in particular, ibid arts 3(8), 28; GDPR, arts 4(7), 26.

35 GDPR, arts 26(3), 82(2).

36 Art 29 Data Protection Working Party, 'Opinion 1/2010 on the concepts of "controller" and "processor"' (n 20) 11–12.

37 Ibid 24.

38 Case C-131/12 *Google Spain and Google* [2014] OJ C 212/4.

39 Ibid para 36.

40 Ibid para 34.

41 Ibid para 40.

42 Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein* [2018] OJ C 268/3.

43 Ibid para 35.

44 Ibid para 36.

45 Ibid para 32.

refer to as 'joint controllership by technical configurations'.

In a later case *Jehovan todistajat*,[46] the Court further expanded the scope to also cover 'joint controllership by organisational configurations'. The Court was asked to clarify, *inter alia*, whether the Jehovah's Witnesses Community should be regarded as a joint controller with its members who collect personal data through door-to-door preaching. An answer was given in the affirmative, on the ground that the 'preaching activity is . . . organised, coordinated and encouraged by that community'.[47] In other words, the mere exertion of organizational influence on how data are processed and for what purposes will suffice to turn an entity into a joint controller.

It is also noteworthy that the Court made it clear that determining the purposes and means of data processing does not necessarily involve 'the use of written guidelines or instructions from the controller'.[48] Nor is it relevant whether the involved party has actual access to the personal data in question.[49] This clearly sets out a broad scope of joint controllers who do not always have to jointly make decisions on the most important aspects of data processing.

In the latest decision, *Fashion ID*,[50] the Court further confirmed how joint controllership may arise regardless of the lack of a legal relationship between the parties concerned, or the absence of access to the personal data by one of them. Like *Wirtschaftsakademie*, the Court was asked to give clarifications on joint controllership with Facebook, but in a different setting: Placing a 'Like' button on one's website that would trigger the user's browser to communicate with Facebook's server and thus make certain information accessible by the latter. The judgment has explained in detail how both the purposes and means are jointly determined by Facebook and the website.

On the one hand, as the Court explains, 'Fashion ID appears to have embedded on its website the Facebook "Like" button made available to website operators by Facebook Ireland while fully aware of the fact that it serves as a tool for the collection and disclosure by transmission of the personal data of visitors to that website'.[51] By including such codes that direct the user's browser to communicate with Facebook, reasons the Court, the website has exercised 'a decisive influence' on the means by which the personal data is processed.[52] On the other hand, Facebook and Fashion ID are held to have jointly determined the purposes of the processing, which is promoting the latter's products 'in the economic interests of both Fashion ID and Facebook Ireland, for whom the fact that it can use those data for its own commercial purposes is the consideration for the benefit to Fashion ID'.[53]

Such joint determination, unlike in *Wirtschaftsakademie*, does not require the operator of the website to sign up for Facebook's service, and thus does not necessarily involve a prior contractual relationship between the parties. Again, all it takes is the technical configurations respectively arranged on both sides following a technical protocol that would altogether enable Facebook to gain access to the personal data in question.

Implications for the smart home ecosystem

From *Google Spain* to *Fashion ID*, there has been an evident and consistent confirmation of the broad scope—if not an expansion of the scope—of joint controllers.[54] Also unmistakably and unmissably clear is the strong message from the case-law that this approach is necessary to ensure a high level of data protection afforded to data subjects.[55] Of course, a widely inclusive notion of joint controllership may arguably hold responsible entities accountable more tightly, and may prevent them from escaping from their data protection duties. However, this may also mean unnecessary or even unfair compliance burden on certain actors involved in, for example, the development and adoption of edge computing technologies, such as Databox and DADA. Such an impact, as will be discussed below, might run counter to certain policy objectives of data protection law, in particular when the responsibilities among stakeholders are not clearly demarcated.

For developers of smart home S/PETs—either the architectural designer of the system or the collaborating or independent developers of certain components—the widening scope of joint controllership means that they may well fall within the definition of a joint controller,

46 Case C-25/17 *Jehovan todistajat* [2018] OJ C 319/7.

47 Ibid para 70.

48 Ibid para 67.

49 Ibid para 69; *Wirtschaftsakademie* (n 42) para 38; Case C-40/17 *Fashion ID* [2019] para 82.

50 *Fashion ID*, ibid. For a detailed analysis of the judgment, see Louisa Specht-Riemenschneider and Ruben Schneider, 'Stuck Half Way: The Limitation of Joint Control after *Fashion ID* (C-40/17)' (2020) 69(2) GRUR International 159.

51 *Fashion ID* (n 49) para 77.

52 Ibid para 78.

53 Ibid para 80.

54 Lilian Edwards and others, 'Data Subjects as Data Controllers: A Fashion(able) Concept?' (2019) <https://policyreview.info/articles/news/data-subjects-data-controllers-fashionable-concept/1400> accessed 9 December 2019.

55 *Google Spain* (n 38) para 34; *Wirtschaftsakademie* (n 42) para 28; *Jehovan todistajat* (n 46) para 66; *Fashion ID* (n 49) para 66.

as they are the ones defining in technical terms how smart home data are collected and for what potential purposes. One might be tempted to argue that under certain technical models where such developers do not have access to the personal data, they may be considered non-controllers. However, as highlighted above, the Court has ruled in several cases that it is irrelevant whether a concerned party has actual access or not to the data when it comes to ascertaining its controllership.[56] This raises an array of questions regarding how data subject rights could be exercised against such controllers when many of those requests—such as access, rectification, erasure—can be fulfilled only when the controller has direct or indirect control over the personal data.

Equally profound are the implications for the users of these technologies, who may find themselves in a dilemma where they make use of such systems in their smart homes in the hope of enhancing privacy or cybersecurity for themselves, their family, their visitors or even the entire infrastructural network, but end up being held liable as a joint controller. From a technical point of view, there is little substantial difference between operating a smart home device that enables data collection and embedding a 'Like' button on a website that triggers data transmission. Keeping smart homeowners in the expanding circle of joint controllers may in individual cases offer some extra protection to data subjects, but this may at the same time create some widespread effects on the adoption of these technologies.

While the WP and the Court seem to have taken into consideration the fair assignment of responsibilities in the case of joint controllership—as will be further discussed below—this would not be effective without further guidance on who should be responsible for what obligations in a given scenario. Before conducting a more nuanced analysis of the allocation of responsibilities, it is necessary to examine some general mechanisms that may serve to push back the expanding boundaries of joint controllership. In the next section, the household exemption will be discussed in detail.

Household exemption: what happens in the house stays in the house?

Even if it is established that a person acts as a data controller, solely or jointly, it does not always follow that the full spectrum of data controller obligations will fall on them. In fact, Article 2 of the GPDR carves out a list of areas from its material scope, one being the household exemption, which could be potentially relevant to the context of smart home security technologies. Article 2(2) GDPR provides that: 'This Regulation does not apply to the processing of personal data: . . . (c) by a natural person in the course of a purely personal or household activity'. Recital 18 further clarifies the meaning of 'a purely personal or household activity' with the qualification of 'with no connection to a professional or commercial activity'. A number of examples are also given in the same recital, which 'could include correspondence and the holding of addresses, or social networking and online activity undertaken within the context of such activities'. Compared with a similar recital in the DPD, which gives examples 'such as correspondence and the holding of records of addresses'[57], the new GDPR recital may seem to have expanded the scope by expressly including social networking and online activities,[58] it should be noted that the GDPR's 'could include' wording may actually suggest a narrower scope than that of the DPD's 'such as'.

The household exemption in a connected and smart home

Before discussing the remit of 'personal or household activity' in the light of these specific examples, and to keep the discussion more focused on the challenging issues, a more straightforward consideration should be pointed out and excluded from our further discussion. In the context of smart home IoT, it is unlikely that the manufacturers of the devices or developers of the software may benefit from this exemption. For one thing, there is a clear professional or even commercial involvement (regardless of their non-/for-profit status) that would rule out the claim of purely personal activity. For another thing, many of these manufacturers or developers are simply not natural persons, but rather organizations, which is also clearly excluded by the exemption. It would be a different question whether they are (joint) controllers, or what responsibilities they have in this case. What is certain, however, is that they can hardly avoid the application of the GDPR by invoking the household exemption. A slightly more reasonable claim may be made by individuals independently contributing to the development of the technologies, but this would

56 *Wirtschaftsakademie* (n 42) para 38; *Jehovan todistajat* (n 46) para 69; *Fashion ID* (n 49) para 82.

57 DPD, recital 12.

58 For the discussions of the applicability of the household exemption to social media users, see Napoleon Xanthoulis, *Negotiating the EU Data Protection Reform: Reflections on the Household Exemption* (2013); Rebecca Wong, 'Social Networking: The Application of the Data Protection Framework Revisited' (2014) 2(2) Birkbeck Law Review 317.

be also hard to justify because, apparently, the use of such technologies concerns, if any, the household *of the user*, not *of the contributors*.

For this reason, the discussion in this part will focus mainly on whether the end users of S/PETs, namely the homeowners, can be exempted from data controller obligations. The CJEU decision on *Ryneš* might be a good starting point for this inquiry as it concerns the use of CCTV—a home security device, albeit not a smart one in this specific case.[59] The Court was asked to decide whether the operation of a CCTV installed on one's home but partly monitoring a public space falls under the household exemption. In the judgment, it is reasoned that:

> [t]o the extent that video surveillance such as that at issue in the main proceedings covers, even partially, a public space and is accordingly directed outwards from the private setting of the person processing the data in that manner, it cannot be regarded as an activity which is a purely "personal or household" activity . . ..[60]

Referring to Recital 18 DPD and by way of example, the Court explains that such an activity may cover 'correspondence and the keeping of address books . . . even if they incidentally concern or may concern the private life of other persons'.[61] Yet, the Court has not further clarified whether it would make a difference if the CCTV is directed entirely towards the inner space of a family home.

However, it is evident that the CJEU has consistently taken a remarkably strict approach to the scope of the exemption. In fact, the Court has never ruled in favour of a claim of the exemption in the limited number of relevant cases it has decided on.[62] In *Jehovan todistajat*, for example, the Court has summarized the two considerations established in previous cases that would preclude the applicability of the household exemption: (a) access by an unrestricted number of people; and (b) extension to a public space beyond the private setting of the person.[63]

In this regard, the question central to the use of S/PETs in a smart home setting would concern the extent to which the use of data is confined to the private sphere of the user and their family. Unlike the case of cameras, however, there is no clear physical boundaries in an IoT setting. While the purpose of the use of these technologies may well be solely for protecting the inner space of home—informationally or physically—the adoption of such measures may, depending on the exact technical model, involve individuals outside the family, either in physical proximity (eg neighbours, visitors) or in the distance (eg other users connected to the same service).

More importantly, the domestic *purpose* or *intention* alone does not form a sufficient basis for the household exemption claim. In *Ryneš*, even though the Court is mindful that the use of CCTV may serve the purpose of protecting one's family, it nevertheless rejects the applicability of the household exemption, and points to alternative permissive mechanisms within the legal framework, such as the 'legitimate interests pursued by the controller, such as the protection of the property, health and life of his family and himself'.[64]

In this regard, it does not seem to matter whether a smart homeowner deploys S/PET devices solely for domestic purposes. The mere fact that such technologies involve collection of personal data from outside the family or dissemination of personal data to outside the domestic sphere will sufficiently exclude the application of the household exemption. The Court's consistent rejection of the claims clearly shows the shrinking possibility for users of these technologies to benefit from the exemption.

Why exempt household activities in the first place? A historical approach

The application of the household exemption means that any data processing falling within the scope of 'a purely personal or household activity' would not be subject to any restrictions imposed by the GDPR. At first glance, many might find this exclusion surprising or even unreasonable: One would expect a highest standard of data protection at home as this amounts to a probably most private and sensitive space. Yet, applying the exemption does not mean that individuals are not protected when it comes to household activities, as any access of data from outside the household that intrude the private sphere of the home would not be considered 'personal' and indeed would be subject to the GDPR. However, this does raise the interesting question as to why such an exemption was introduced in the first place.

The earliest equivalent to today's definition of the household exemption can be found in Sweden's 1982 Amendment to the Data Act 1973, which provides that the prior approval and reporting requirements for data

59 Case C-212/13 *Ryneš* [2014] OJ C 46/6.

60 Ibid para 33.

61 Ibid para 32.

62 Case C-101/01 *Lindqvist* [2003] OJ C 7/3; Case C-73/07 *Satakunnan Markkinapörssi and Satamedia* [2008] OJ C 44/6; *Ryneš* (n 59); *Jehovan todistajat* (n 46).

63 *Jehovan todistajat* (n 46) para 42.

64 *Ryneš* (n 59) para 34.

registers do not apply to 'personal data registers established by an individual or exclusively for personal use'. [65] In the explanatory notes, this was justified on the ground that 'it is not possible to regulate all forms of use of personal data that normally occur in the daily interactions between people, e.g. in private notes, address or phone number lists, and letters etc'.[66] as well as 'registers relating to one's own family finances'.[67]

On the international level, the updated version of Convention 108 adopted in 2018 ('Convention 108+') includes a clear household exemption. In the new Article 3(2), it is provided that '[t]his Convention shall not apply to data processing carried out by an individual in the course of purely personal or household activities'. A rationale has been given in the Explanatory Report:

> This exclusion aims at avoiding the imposition of unreasonable obligations on data processing carried out by individuals in their private sphere for activities relating to the exercise of their private life. ... The sharing of data within the private sphere encompasses notably the sharing between a family, a restricted circle of friends or a circle which is limited in its size and based on a personal relationship or a particular relation of trust.[68]

As regards the EU, the original Commission proposal of the DPD offers a justification of excluding the application to 'files held by ... an individual solely for private and personal purposes'[69]: '[I]nvasions of privacy are unlikely to occur ... because the data are used for private purposes only, as is the case with a personal electronic diary'.[70] Indeed, considering the potential risks in such scenarios, it would be significantly disproportionate to require individuals to comply with data protection law, including allowing data subjects access to the data, just because their personal details are mentioned in an e-diary.

Even more interestingly, in the same proposal, another account was provided in the draft Recital 9 (which did not make its way to the Council's Common Position[71]): '[D]ata files falling exclusively within the confines of the exercise of a natural person's right to privacy, such as personal address files, must be excluded'.[72] While closely related to the point mentioned in the previous paragraph, this explanation has taken a somewhat different approach: Applying data protection law to purely personal activities is not just unnecessary for protecting the data subject, but also potentially intrusive for the individuals keeping such data,[73] as it would potentially force them to disclose highly sensitive materials at the request of the data subject.

To sum up, from the limited number of official documents providing an explanation to the introduction of a household exemption, three inseparable but somewhat different theories can be identified: Data protection law should not apply to purely personal or household activities because it would be (i) *unfair*, as it would impose unreasonable obligations to the data controller; (ii) *unnecessary*, as the privacy threats are minimal in these cases; and (iii) *invasive*, as it would risk forcing individuals to disclose confidential information.

When joint controllership and the household exemption face a smart home: do they still work?

Joint controllership and the household exemption as mechanisms for allocating responsibilities

In the two previous sections, it has been shown how the scope of joint controllership has been widening whereas the scope of the household exemption has been narrowing as the two concepts have been interpreted by the CJEU. Consequently, for owners of smart homes, choosing to embrace a technology designed to improve the security and privacy of their homes may mean a high risk of being categorized a joint controller and without the protection afforded by the household exemption.

65 Lag (1982:446) om ändring i datalagen (1973:289) [1982], § 2, para 3 (self-translation). Original text of a consolidated version can be found at <https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/datalag-1973289_sfs-1973-289> accessed 9 December 2019.

66 , 'Regeringens proposition 1981/82:189 om ändring i datalagen (1973:289) m. m.' (1982) 23 <https://www.riksdagen.se/sv/dokument-lagar/dokument/proposition/om-andring-i-datalagen-1973289-mm_G503189> accessed 15 April 2020 (self-translation).

67 Ibid 54 (self-translation).

68 Council of Europe, 'Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data' (2018) 5.

69 Commission, 'Proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data' (1990) 314 final—SYN 287.

70 Ibid.

71 Council, 'Common Position (EC) No 1/95 adopted by the Council on 20 February 1995 with a view to adopting Directive 95/. . ./EC of the European Parliament and of the Council of ... on the protection of individuals with regard to the processing of personal data and on the free movement of such data' (1995) 95/C 93/01.

72 Commission, 'Proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data' (n 69).

73 See also Rebecca Wong and Joseph Savirimuthu, 'All or Nothing: This Is the Question? The Application of Article 3(2) Data Protection Directive 95/46/EC to the Internet' (2008) XXV Journal of Computer & Information Law 241.

Joint controllership and the household exemption, although as two separate legal issues, are closely linked here since the former sets out the threshold whereby a group of entities are made collectively responsible for the data processing, whereas the latter functions in a way that essentially exempts the individuals processing personal data from controllership if the activities in question are purely personal or domestic. The GDPR further clarifies that the exemption applies only to natural persons but not to the entities providing means for such activities.[74] Accordingly, with regard to the processing involved in the sending of private messages on social media, for example, the senders and receivers may be exempted from the application of the GDPR, but the social media service provider will not. In other words, the household exemption is a controller-specific exemption that seeks to relieve private individuals from the compliance burdens.

For this reason, the notion of joint controllership and the household exemption are in essence an all-or-nothing mechanism by precluding the responsibilities for some groups of data users, and thus imposing them exclusively on some other groups.[75] Working together, these two concepts follow the logic that, if a person is a data controller and unqualified for the household exemption, then they will be charged with the full responsibilities (or as a part of a full package of responsibilities); otherwise, they will have no responsibility at all. The responsibilities of each joint controller, as explained below, may not be identical, but without clear guidance, joint controllership may lead to a considerable amount of burdens that are not proportionate to the role of each controller. To the extent that joint controllership and the household exemption determine who should and who should not be held responsible for data processing activities, they serve as a legal mechanism to assign responsibilities.

This marks a fundamental difference underlying privacy and data protection law: while privacy law focuses more on the secrecy of personal and private information, data protection law mainly addresses the accountability of uses of personal data.[76] As much as confidentiality forms an important part of accountability, the latter is achieved also through other mechanisms, such as integrity, availability, transparency and so on. One important aspect of a data protection regime is thus to determine the extent to which the responsibilities are distributed—or rather, centralized—among various stakeholders. By setting out the household exemption, for instance, EU data protection law has in effect removed the responsibilities from individuals when using personal data for purely personal activities. Indeed, individuals are expected to be subject to a much lower level of accountability when they engage in a conversation with family and friends, or handling personal details of family members within the household.

The way joint controllership and the household exemption are laid down in the GDPR reflects a few assumptions that might be valid for a traditional home but probably not anymore for a smart home. First, it is assumed that personal or domestic activities are mostly confined within the physically discernible boundaries of a private space. The keeping of an address book,[77] for example, usually operates solely within one's home and thus has little, if any, impact on the listed contacts. Secondly, responsibilities can be clearly defined and simply assigned or *dis*assigned to a specified group of persons. In the case of an address book, again, the book-keepers would be the only parties responsible for the use of the address book, which does not involve the issues of shared responsibilities. Under these two conditions, the two notions may work well in a straightforward manner: Within the house, no responsibility; outside the house, full responsibility. However, as will be shown in the rest of this section, these two assumptions do not work in an IoT context anymore.

In or out: disappearing boundaries of the home

There should be little dispute that the examples provided by Recital 18 GDPR— ie 'correspondence', 'holding of addresses'—can be reasonably exempted from the application of data protection law since the imposition of the obligations on individuals in these contexts would be, as highlighted above, unfair, unnecessary and invasive. Private messages mentioning a third-party individual solely for personal purpose, for instance, should not result in the mentioned person given the right to access the information. Again, this does not mean that the information involved in such activities is unprotected. Confidentiality of communications, whether in postal or electronic forms, remains protected by (e-)privacy law.

74 GDPR, Recital 18.

75 Brendan Van Alsenoy, 'Regulating Data Protection: The Allocation of Responsibility and Risk Among Actors Involved in Personal Data Processing' (KU Leuven 2016).

76 Orla Lynskey, 'Deconstructing Data Protection: The "Added-value" of a Right to Data Protection in the EU Legal Order' (2014) 63 International and Comparative Law Quarterly 569.

77 See GDPR, Recital 18.

This is underpinned by the idea that certain spaces can be clearly demarcated as private or personal, and thus what happens within such spaces should be free from interference. Interestingly, though, the two examples provided by Recital 18 in fact represent two quite different types of private space, and not necessarily limited to the physical household. Koops distinguishes 'home' and 'private communications' as two different types of 'intimate zones'.[78] Whereas 'holding of addresses' can be considered within the 'home' space, 'correspondence' clearly falls within the 'private communications' space. Yet, these two instances share the similarly visible infrastructural boundaries that afford a relatively high level of assurance that the information contained within such boundaries—what happens inside the house, or what is written inside the envelope—would not reach the outside world and would thus have little external impact. Unless intentionally intruded or disclosed, which clearly breaches the private space, the expectation of what should stay private and thus subject to a significantly lower level of accountability is rather clear.

There is a rich body of literature discussing the importance of boundary management under the heading of 'privacy'.[79] Non-smart homes and non-electronic communications in most cases have more manageable boundaries as they are clearly defined and visible to all parties. Setting aside the question whether privacy is a helpful approach here,[80] what should be less disputable is the challenge to boundary management posed by the increasing prevalence of IoT technologies. The boundaries of a smart home are remarkably more fluid as smart devices may—and, sometimes indeed, are designed to—transmit information about what is happening inside the home to the remote cloud. Also, the internal functioning of a smart home may be affected by or even dependent on events taking place outside the home. Even more fundamental, IoT technologies pose challenges to what is traditionally considered trusted as part of one's home.[81] Unlike a non-smart home, the relational and informational boundaries have disentangled from the physical boundaries.[82]

This is particularly the case in the scenarios central to this article, ie S/PETs operating on an open-source, data-intensive and dynamic basis, such as Databox or DADA. Depending on the exact design of the system, a smart home security solution may, for example, record the presence of detected new devices, which could be brought into or close to the house by visitors or neighbours.[83] Unlike using a physical domestic diary to keep record of guests, such a system may store more details of the device or reveal certain patterns. In most cases, the communication and storage of information would be secure, but it is certainly not as straightforward as a paper diary book, and family members, visitors, neighbours might have concerns over the safety of such information. The functioning of devices may also be affected by what is happening outside the home. The system may decide, for instance, to disconnect a device from the network after identifying suspicious pattern matching a newly reported cyberattack.

In a hyper-connected setting like a smart home, it is no longer clear whether the involved parties—the homeowner, their family, their neighbours, their visitors, other connected users, operators of the devices, cloud providers—should be considered 'inside' or 'outside' the home. Or maybe more fundamentally, we might need to reflect on the appropriateness of the metaphor of a traditional house—perhaps the external and internal spheres are no longer separated by a thin wall, but rather bridged by a spectrum of domains with different levels of proximity to the core of the home, and thus carrying different expectations of accountability.[84]

78 Bert-Jaap Koops, 'Privacy Spaces' (2018) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3157169> accessed 9 December 2019.

79 For an overview, see Leysia Palen and Paul Dourish, 'Unpacking "Privacy" for a Networked World' (SIGCHI Conference on Human Factors in Computing Systems, Ft. Lauderdale, Florida, 5-10 April 2003); Andy Crabtree, Peter Tolmie and Will Knight, 'Repacking "Privacy" for a Networked World' (2017) 26(4–6) Computer Supported Cooperative Work (CSCW) 453.

80 Crabtree, Tolmie and Knight (n 79).

81 Nicole Newmeyer, 'The Impact of IoT Devices on Network Trust Boundaries' in Tyson T Brooks (ed), *Cyber-Assurance for the Internet of Things* (IEEE Press, Piscataway 2017).

82 For example, smart home users have new ways to manage their relational boundaries, including password sharing Crabtree, Tolmie and Knight (n 79) and other forms Alison Burrows, David Coyle and Rachael Gooberman-Hill, 'Privacy, Boundaries and Smart Homes for Health: An Ethnographic Study' (2018) 50 Health & Place 112.

83 This can be revealing in terms of surfacing domestic politics. See Marshini Chetty and others, 'Who's Hogging the Bandwidth: The Consequences of Revealing the Invisible in the Home' (SIGCHI Conference on Human Factors in Computing Systems, Atlanta, Georgia, 10–15 April 2010).

84 Urquhart et al have explored a similar idea with reference to Brand's Shearing Layers in an Adaptive Architecture Lachlan Urquhart, Holger Schnädelbach and Nils Jäger, 'Adaptive Architecture: Regulating Human Building Interaction' (2019) 33 International Review of Law, Computers & Technology 3. The idea of going beyond the private/public dichotomy is also discussed in Lilian Edwards and Lachlan Urquhart, 'Privacy in Public Spaces: What Expectations of Privacy Do We Have in Social Media Intelligence?' (2016) 24 International Journal of Law and Information Technology 279.

To such an extent, a smart home may even be seen as a digital 'private-public place'.[85]

This points towards the need for further user-centric research on user expectation and experiences in a smart home equipped with S/PET systems, but from a legal point of view, the assumption that a relatively clear line can be drawn between the domestic and public spaces will only become increasingly unrealistic.[86]

All or nothing: centralized data controllership in a decentralized technological reality

In a simple, one-to-one legal relationship, the GDPR's centralized model mirrored in joint controllership and the household exemption[87] have the benefit of allowing for a clear focal point of obligations largely reflecting the expected roles of the parties involved. When it comes to a highly complex technological setting, however, it does not seem fair anymore to distribute the duties of care in an all-or-nothing manner. The example of S/PETs discussed in this article serves as a good case in point: Such technologies rely on the collaborative involvement of a range of actors who have different roles to play, and thus have different level of control over the functioning of the system.

We propose to use functional terms to capture the nature of control exercised by a variety of actors. The developers of the system, for example, have *schematic control* as they determine the structure of data and protocols mandating the communications between components across the system, but they have no access to the actual data; the device manufacturers have *input control* as they determine what data are collected and transmitted through the network; the developers of drivers or apps have *interpretative control* as they determine how data or data pattern can be translated into actionable decisions; the users (homeowners) have *operational control* as they determine what components or functionalities are enabled. As a preliminary example, however, this taxonomic approach will certainly require further theoretical and practical elaboration.

The level of integration and inter-dependency between various types of actors means that accountability is shared, not just in proportional/quantitative terms but also in a functional/qualitative manner. The operational control by the users naturally requires them not to abuse the system by, say, monitoring the digital activities of their neighbours; the input control by the manufacturers requires them not to over-collect data; the schematic control by the developers requires them not to make unauthorized data sharing possible between different components. Sitting in different functional divisions of the system, they are in position for different forms of accountability. Particularly important are the asymmetries in resources and power reflected in different forms of control and the implications for regulation. The simple answer offered by joint controllership and the household exemption, however, seems to have failed to reflect such a complex landscape. The idea of differentiated responsibilities as envisaged by the WP and the CJEU—which will be discussed in the next section—may mitigate this issue to some extent, but certain challenges remain.

In this regard, the GDPR contains a provision that is highly relevant but remarkably under-discussed: Recital 78 provides that 'producers of the products, services and applications should be encouraged to take into account the right to data protection . . . with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations'. It sheds some light on the roles that the involved parties are expected to assume in the collaborative process of improving security/privacy for smart homes. Interestingly though, it seems these producers are not categorized as data controllers (or at least implying that they can be treated as non-controllers in some contexts) as they are simply 'encouraged' but not 'obliged' (as the case would be for a controller) to take into account the rights of the data subjects. In the case of S/PETs for smart homes, the contributors to some components are technically not data controllers indeed—due to the fact that, say, they do not actually determine the overall purpose of the system but simply offer a partial technical solution to the community. Yet, it does not follow that they do not have any control over how data are eventually processed. It equally does not follow that it would be fair to impose the full range of data controller obligations on them. In determining to what degree and in what form they should act responsibly and how such responsibilities should be translated into legal obligations, maybe it would take more than an answer of yes or no.

The same goes for the owner of a smart home equipped with such technologies—they have a certain level of control over the use of data for purposes that

85 Lilian Edwards, 'Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective' (2016) 2(1) European Data Protection Law Review 28.

86 See also Zuzanna Warso, 'There's More to It Than Data Protection - Fundamental Rights, Privacy and the Personal/Household Exemption in the Digital Age' (2013) 29 Computer Law & Security Review 491.

87 René Mahieu, Joris Van Hoboken and Hadi Asghari, 'Responsibility for Data Protection in a Networked World: On the Question of the Controller, "Effective and Complete Protection" and its Application to Data Access Rights in Europe' (2019) 10 JIPITEC 85.

might be largely but not necessarily entirely 'personal or household'. In order to decide the extent to which the exemption should apply to them, one would need to go back to the three questions that the early legislator adopting the household exemption might have asked themselves: Is it *fair* to impose the data controller obligations on them? Is it *necessary* to do so taking into account the potential risks? Is it *invasive* to do so considering the implications for the homeowner and their family? The three answers may not be fully consistent anymore. Perhaps more importantly, in a world of decentralized control over data processing, and possibly diffused responsibilities among entities,[88] these questions might well be a matter of balance rather than one of choice.

Differentiated responsibilities among joint controllers: promises and limitations

One might argue that the expanding scope of joint controllership and the shrinking scope of the household exemption do not necessarily mean disproportionate obligations imposed on certain groups of actors. Indeed, Article 26(1) of the GDPR requires that joint controllers should 'in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation . . . by means of an arrangement between them'.[89] Also, while this requirement is newly introduced by the GDPR, during the time of the DPD, the WP as well as the CJEU have already expressed some support to such a possibility.

The A29 WP has indeed anticipated the need to ascertain 'which controller is competent – and liable – for which data subjects' rights and obligations . . . where the various joint controllers share purposes and means of processing in an asymmetrical way'.[90] While the WP has not ruled out the possibility of joint and several liability—ie each and all joint controllers fully liable for any breach arising from the data processing—it has pointed out that in most cases 'the various controllers maybe be responsible – and thus liable – for the processing of personal data at different stages and to different degrees'.[91]

This interpretation has later been confirmed by the Court in *Wirtschaftsakademie*, which states that 'the existence of joint responsibility does not necessarily imply equal responsibility of the various operators involved in the processing of personal data' and that 'those operators may be involved at different stages of that processing of personal data and to different degrees, so that the level of responsibility of each of them must be assessed with regard to all the relevant circumstances of the particular case'.[92] This approach is subsequently reaffirmed by the Court in both *Jehovan todistajat*[93] and *Fashion ID*.[94]

As explained above, it is indeed reasonable and necessary to differentiate the obligations of different controllers taking into account their respective roles in the whole process of determining the purposes and means of data processing. However, the approach proposed by the WP, later confirmed by the Court and then adopted by the GDPR is subject to a number of challenges.

Firstly, the current mechanism is largely based on the assumption that joint controllers have or can come to agree on how the responsibilities should be distributed among themselves. In fact, as mentioned above, data controllers are required to do so under the GDPR 'by means of an arrangement between them'.[95] Yet, our analysis in the section on joint controllership above has shown that the establishment of controllership does not require a legal arrangement between the concerned parties, and can simply result from technical or organizational configurations. Even if it is argued that such an arrangement can and should be concluded, in the context of open-source development, this would be highly difficult.[96]

Secondly, both the WP and the Court have considered the possibility of joint controllers as a result of data processing 'at different stages' or 'to different degrees', and thus the 'level of responsibility' should be differentiated. This solution essentially views the distribution of data protection responsibilities as a matter of degree in temporal or proportional terms, which would make sense in allocating *ex post* responsibilities—ie liabilities. Van Alsenoy, for example, analyses the liabilities of data

88 See Christopher Millard and others, 'At This Rate, Everyone Will Be a [Joint] Controller of Personal Data!' (2019) 9(4) International Data Privacy Law 217.

89 GDPR, art 26(1).

90 Art 29 Data Protection Working Party, 'Opinion 1/2010 on the concepts of "controller" and "processor"' (n 20).

91 Ibid.

92 *Wirtschaftsakademie* (n 42) para 43.

93 *Jehovan todistajat* (n 46) para 66.

94 *Fashion ID* (n 49) para 70.

95 GDPR, art 26(1).

96 Mahieu, Van Hoboken and Asghari (n 87).

controllers and data processors from a tort law perspective.[97] The joint and several liability approach, for example, can be supported by Recital 146[98] and justified with the 'common fault' theory,[99] although the GDPR exempts controllers who can prove 'not in any way responsible'.[100] However, unlike tort law, data protection law concerns not only *ex post* liabilities, but also *ex ante* duties, including the mandatory conditions for lawful processing of personal data and other safeguards throughout the personal data lifecycle. The way liabilities are distributed among responsible parties, often ascertained in monetary form and as a matter of degree, would not be suitable for allocating *ex ante* duties. As highlighted in the previous section, different forms of control (eg schematic, input, interpretative, operational, etc) would put joint controllers in different positions to adopt different measures, which is a matter not the same as 'different stages' or 'different degrees'. In any case, the default approach of joint and several liability is certainly unhelpful in assigning data protection responsibilities fairly.

Thirdly, it remains unclear how to reconcile what seems to be a conflict[101] between the requirement to determine the responsibilities among joint controllers[102] and the proviso that data subject rights can be exercised against any of the joint controller.[103] One potential solution rests in Article 26(2), which requires the arrangement between joint controllers to 'duly reflect the respective roles and relationships of the joint controllers *vis-à-vis* the data subjects'.[104] This can be interpreted as allowing joint controllers to appoint one of them to be responsible for certain types of data subject rights, as long as this mirrors its role and relationship with the data subject; otherwise, the data subject would not be bound by such a designation and may decide to exercise their rights against any of the controllers.[105]

In practice, some of these challenges may be slightly mitigated by restricting the ways data subject rights may be exercised against some of the joint controllers. Article 23 of the GDPR allows Member State laws to set out such restrictions on a number of bases, including safeguarding 'the protection of the data subject or the rights and freedoms of others'.[106] The security and privacy interest of the homeowners, for instance, may be recognized by national laws against the rights of the data subjects. Making these rules, however, would require a strong justification based on fair allocation of responsibilities, and may risk creating further fragmentation among Member States.

The lack of legal certainty on these matters may significantly impede the development and adoption of smart home technologies that would enhance privacy and security for IoT users. Fair allocation of data protection responsibilities would entail going beyond the current approaches of joint controllership and the household exemption, and instead, investigating what role each of the participating parties is playing, and accordingly, what appropriate duties they should be expected to assume.[107] Much work is needed to map out different categories of actors in the domestic IoT ecosystem in order to ascertain their best position in the data protection regime. Since it is now part of the EDPB's plan to review the WP's Opinion on controller and processor,[108] the need to carry out further research, both theoretically and empirically, will become even more pressing.

Conclusion

Before the advent of smart home IoT technologies, ascertaining how data protection law should regulate users in a domestic setting was once straightforward; the burdens of domestic data controllers were alleviated by relieving them of the data protection responsibilities. This is not the case anymore. The use of cases discussed throughout this article have shown how domestic IoT has challenged some of the underlying assumptions of data protection law, and has created legal uncertainties as to who should assume the primary responsibility among a group of stakeholders connected to the smart home edge computing architectures, as well as how accountability can be achieved in a coordinated and shared manner between them.

97 Brendan Van Alsenoy, 'Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation' (2016) 7 JIPITEC 271.

98 Valentina Colcelli, 'Joint Controller Agreement under GDPR' (2019) 3 EU and Comparative Law Issues and Challenges Series 1030.

99 Van Alsenoy, 'Liability under EU Data Protection Law' (n 97).

100 GDPR, art 82(3).

101 See *Fashion ID* (n 49) Opinion of AG Bobek, para 80.

102 GDPR, art 26(1).

103 Ibid art 26(3).

104 Ibid art 26(2).

105 See art 29 Data Protection Working Party, 'Opinion 1/2010 on the concepts of "controller" and "processor"' (n 20) 24.

106 GDPR, art 23(1)(i). For a discussion on how this can be applied to a context of freedom of expression, see David Erdos, 'Beyond "Having a Domestic"? Regulatory Interpretation of European Data Protection Law and Individual Publication' (2017) 33 Computer Law & Security Review 275.

107 For a discussion of allocating data protection responsibilities with a number of use cases, see Van Alsenoy, 'Regulating Data Protection' (n 75).

108 European Data Protection Board, 'EDPB Work Program 2019/2020' (2019) <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-02-12plen-2.1edpb_work_program_en.pdf> accessed 9 December 2019.

This raises the fundamental issue of how data protection law should regulate smart homes. The expanding scope of joint controllership and the shrinking scope of the household exemption, as discussed above, are intended to ensure a high degree of accountability, and to ensure data subjects always have someone to answer for their requests. Important as this consideration is, the current interpretative approach may end up unfairly burdening certain stakeholders in smart homes and thus disincentivise uptake of edge computing solutions such as Databox and DADA. Paradoxically this may then result in a *lower* degree of privacy, as well as security, for smart home inhabitants.

We argue that this issue goes beyond mere black letter law interpretation of the GDPR. Further research is needed to conceptualize the control of various natures exercised by different stakeholders in smart IoT systems. Normatively, an analytical framework should be developed to situate stakeholders according to the influence they have in ensuring collective accountability with others. Empirically, further evidence is required for a better understanding of the power dynamics among stakeholders with asymmetric resources and various control, as well as public perceptions of what amounts to fair reassignment of responsibility and accountability in a domestic IoT context. All these considerations, if properly explored and translated across disciplines—computer science, law, human-computer interaction, and ethnomethodology[109]—will inform both the design of future IoT systems or S/PETs and the creation of the wider regulatory environment to support those developments.

doi:10.1093/idpl/ipaa011

109 For the latest research in this field, see Murray Goulden, '"Delete the Family": Platform Families and the Colonisation of the Smart Home' (2019) Information, Communication & Society 1.